6 - Security

Sample

[5 Marks] Why symmetric keys are used for traffic encryption instead of asymmetric keys? Explain how asymmetric keys are used in digital signatures.

Asymmetric keys consume more resources than symmetric keys. Since the traffic is very busy in the internet world, using asymmetric encryption will hugely increase the computational cost. Therefore, it is generally applied to distribute the symmetric keys at start.

Digital signatures: P102

21S1

Q3: Describe five types of attacks (on processes, communication channels, services) that might occur in the Internet. P95

- Eavesdropping (窃听) - A form of leakage
    - Obtaining private or secret information or copies of messages without authority.
- Masquerading (伪装) - A form of impersonating
    - Assuming the identity of another user/principal
    - Sending or receiving messages using the identity of another principal without their authority.
- Message tampering - altering the content of messages in transit
    - Man in the middle attack (tampers with the secure channel mechanism).
- Replaying
    - Storing secure messages and sending them at a later date.
- Denial of service - Vandalism (DDOS)
    - Flooding a channel or other resource, denying access to others.
    - Deliberately excessive use of resources to the extent that they are not available to legitimate users.

Q8: Why is symmetric encryption used for session encryption, rather than asymmetric encryption? Explain how asymmetric keys are used in digital signatures.

Asymmetric keys consume more resources than symmetric keys. Since the traffic is very busy in the internet world, using asymmetric encryption will hugely increase the computational cost. Therefore, it is generally applied to distribute the symmetric keys at start.

Digital signatures: P102

Q9: Discuss the secure socket layer (SSL) with Transport Level Security (TLS) protocol stack architecture and its components.

P107 / L6 P32

This is intended to provide a flexible way for clients and server to communicate using a secure channel, preventing potential attacks.

There are 3 basic phases:

- Peer negotiation for algorithm support
- Public key encryption-based key exchange and certificate-based authentication
- Symmetric cipher-based traffic encryption

Q12.8: Which of the following technology supports dynamic negotiation of encryption and authentication algorithms?

- Secure Socket Layer ✔
- Kerberos
- Firewall
- Certificate Authority

17S1

Q(5): (a) [4 marks] What is the purpose of cipher block chaining? Describe a technique that achieves cypher block chaining.

Cipher block chaining (CBC) is **a mode of operation for a block cipher -- one in which a sequence of bits are encrypted as a single unit, or block, with a cipher key applied to the entire block**. Cipher block chaining uses what is known as an initialization vector (IV) of a certain length.

(b) [3 marks] List and briefly explain three worst-case assumptions when designing a secure system. P95

- Leakage
- Tampering
- Vandalism

(c) [3 marks] Explain what is a digital certificate, including what is the basic technique used to create a digital certificate, and what is a certificate chain.

L6 P22

A digital certificate is used to certify the user's identity, which can be issued by certificate authorities.

16S2

Q7: (a) [2 marks] Some distributed systems, such as secure shell, require the user to explicitly trust a public key provided by the server, when connecting for the first time. Name the security risk that this presents and explain why this is a security risk.

- The system may be a fake one so that users' information may be leaked.
- The real system may have huge loss since the fake one has provided the services on behalf of it.

(b) [3 marks] Explain what is meant by challenge-response and give an example of its use. L6 P17

The challenge-response technique is now widely used to avoid sending passwords in the clear. The identity of a client is established by sending the client an encrypted message that only the client should be able to decrypt, this is called a challenge message. If the client cannot decrypt the challenge message then the client cannot properly respond.

Example: Password authentication, CAPTCHA: distinguish between humans and bots

15S2

Q6: (a) [1 marks] What is a digital signature? L6 P19

A digital signature serves the same role as a signature, binding an identity to a message.

(b) [1 marks] When constructing a digital signature can we use a symmetric or asymmetric encryption algorithm or both? P102

Asymmetric encryption is used.

(c) [1 marks] Why is a digital signature non-reputable?

Because only the user with the signature has the private key to encrypt.

(d) [1 marks] What key pieces of information in a digital certificate are signed using a digital signature?

The certificate is signed by the issuer (certificate authority).

(e) [2 marks] Known threats can be listed and the designer can show how the distributed system offers security against such threats. What can be done about unknown threats?

Leakage: Verify the digital certificate first

Tampering: Use TLS to transfer messages

Vandalism: Use DDoS protection (Anti-DDoS IP)